BlueFantasy, Virus Lokal yang Menyebar Lewat CD

Perkembangan virus komputer saat ini sedang ramai-ramainya. Apalagi setelah apa yang dilakukan oleh Brontok, yang dalam waktu belakangan ini menjadi sangat tenar di kalangan pengguna komputer, karena penyebarannya yang sangat hebat. Akibatnya sekarang banyak sekali virus *made in* lokal yang bermunculan. Salah satunya adalah virus BlueFantasy. Seperti apa *sih* si BlueFantasy ini?

Arief Prabowo

Kemunculan virus BlueFantasy ini memang belum seheboh virus Brontok. Tapi karena Brontok jugalah, yang akhirnya memicu para programer lokal untuk berlomba-lomba memproduksi virus yang hebat. Tujuan atau maksud dari pembuat virus pun bermacam-macam, tapi yang jelas, apapun tujuan dari pembuat virus itu, yang pasti kita telah dirugikan oleh virus-virus buatan mereka.

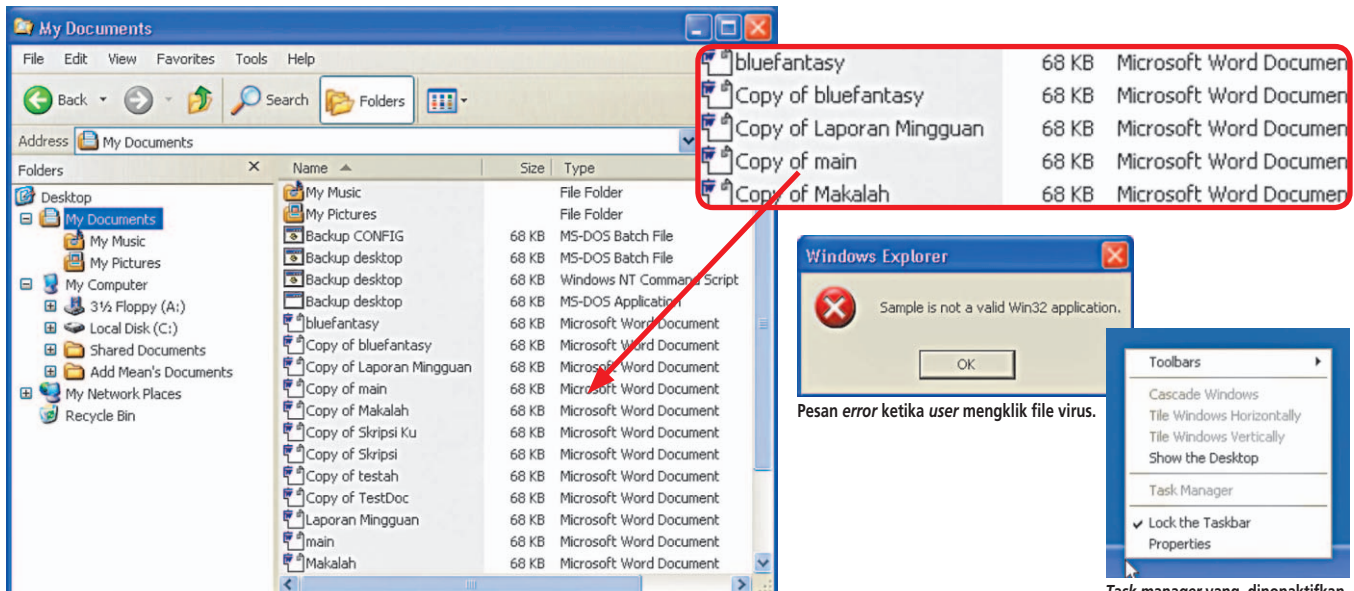
BlueFantasy, virus *made in* lokal yang satu ini, memang boleh dibilang sederhana. Teknik kompresi dan enkripsi tidak terdapat pada virus ini. Walaupun begitu, virus ini juga dapat membuat kita kerepotan.

Bentuk Fisik

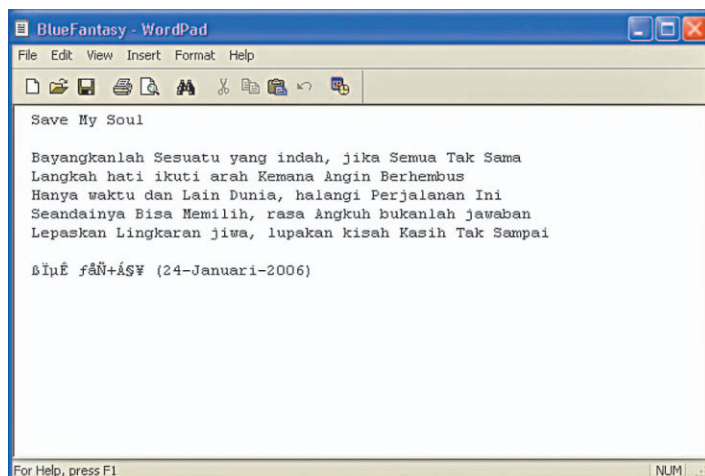
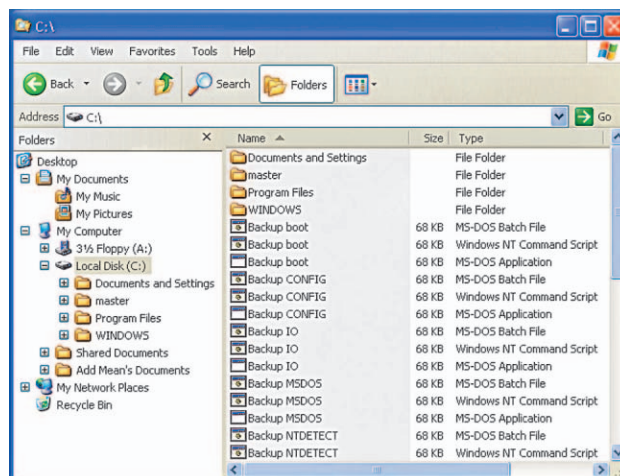
Virus yang dapat menginfeksi *operating system* berbasis Windows 9x dan XP ini menyamar sebagai dokumen Microsoft Word, karena icon yang digunakan sama seperti pada Microsoft Word. Trik ini juga pernah dilakukan oleh pendahulunya, yaitu virus Kangen/Pesin. Mungkin beberapa dari Anda pernah mengalaminya, ketika mencoba mengklik file yang Anda kira adalah file dokumen Microsoft Word, namun setelah diklik ternyata dia hanya menampilkan pesan *error* berupa *message box* dengan tulisan "....is not a valid win32 application". Apabila itu terjadi, Anda harus memeriksa komputer Anda, karena kemungkinan komputer telah terinfeksi oleh virus BlueFantasy.

Bagaimana Ia Menginfeksi?

Virus ini dapat menyebar melalui media penyimpanan portable seperti flash disk, cd, ataupun disket. Pada saat pertama kali virus dieksekusi, ia akan segera menginfeksi komputer tersebut dengan meng-*copy*-kan dirinya ke beberapa direktori penting, diantaranya pada direktori System menggunakan nama Win32.com dengan *attribut hidden*, juga pada *Desktop, My Documents,* dan *StartUp Folder* dengan nama file sama seperti yang dieksekusi.

Virus ini juga cukup merepotkan. Bagaimana tidak, virus ini secara *real time* akan membaca direktori aktif, misalkan Anda sedang melakukan *browsing* direktori pada Windows Explorer, maka virus akan mencari file apa saja yang terdapat pada direktori tersebut, lalu membuat duplikat dari dirinya dengan memanfaatkan nama file yang ditemukannya, hanya saja ditambahkan kata-kata *Backup, Shortcut to*, atau *Copy of,* dengan ekstensi yang juga berbeda-beda, bat, com, pif, scr, atau exe.

Dokumen Word asli disembunyikan dan diganti dengan file virus.

Pesan *error* ketika *user* mengklik file virus.

Task manager yang dinonaktifkan oleh BlueFantasy.

Pesan dari si pembuat virus yang dikutip dari penggalan judul-judul lagu "Padi".

BlueFantasy membuat duplikat dirinya dengan menggunakan nama file yang ada.

Sementara untuk file dokumen .doc Anda, virus akan menyembunyikan file aslinya dan mengganti dengan dirinya sendiri menggunakan nama file .doc yang asli. Mungkin tidak masalah apabila pada direktori tersebut hanya terdapat 2-3 file, tapi bagaimana dengan 100 atau 1000? *Kebayang kan* bagaimana merepotkannya? Apabila kita coba hapus file-file virus tersebut, tidak akan berhasil, karena virus akan terus membuat duplikat atas dirinya, lagi, lagi, dan lagi.

Aktif di Memory

Virus akan selalu aktif setiap kali memulai Windows. Karena ia telah menginfeksi *registry* dan StartUp folder agar Windows selalu menjalankan virus ini.

Registry key yang diinfeksi adalah pada HKLM\Software\Microsoft\Windows\CurrentVersion\Run dengan ditambahkannya String Value dengan nama "Task Scheduler" yang berisi "Win32". Maksud dari *value* tersebut mengarah kepada file copy-an dari virus, yakni Win32.com yang terdapat pada direktori System. Melalui Win32.com ini, virus akan selalu aktif di memory, dan akan selalu memonitor kegiatan Anda.

Virus juga memanfaatkan StartUp folder sebagai media untuk melakukan *autorun*. Dan file-file virus yang berada pada StartUp folder tersebut berasal dari setiap file virus yang Anda klik.

Apabila Anda ingin mematikan proses dari virus BlueFantasy ini dengan melakukan "End Process" dari Task Manager, juga "Tasklist" dan "Taskkill" pada Windows XP tidak dapat dilakukan karena itu semua telah diblok oleh BlueFantasy.

Apa Saja yang Dilakukannya?

Seperti halnya yang dilakukan oleh virus-virus lain, Brontok contohnya, BlueFantasy akan membaca *caption* dari setiap program, apabila mengandung kata-kata seperti contohnya REGIS, CONFIG, TASK, dan NORTON, maka dengan sigap BlueFantasy akan menutupnya. Ini dilakukannya agar tetap dapat melangsungkan hidupnya. Registry juga selalu menjadi sasaran empuk para virus, ini berlaku juga untuk BlueFantasy, selain menonaktifkan Registry Editor, virus ini mengubah *extension information* dari setiap file .exe dan .scr menjadi "Microsoft Word Document".

Ini dapat Anda buktikan ketika Anda membuka Windows Explorer, dan set tampilan view menjadi *Details*. Anda akan melihat bahwa semua file executable akan bertipe sebagai "Microsoft Word Document". Anda juga tidak akan menemukan beberapa menu pada *Start Menu>Settings*, karena virus ini juga menyembunyikannya.

BlueFantasy juga mengubah *setting*-an dari file msdos.sys, sehingga pada saat *booting* akan menampilan *warning* untuk *Safe-Mode*. Hanya saja Anda tidak akan bisa masuk ke Safe-Mode karena akses tombol F5, F6, atau F8 juga dinonaktifkan oleh virus ini. Tapi, ini hanya berpengaruh apabila operating system yang Anda gunakan berbasis Windows 9x.

Jangan kaget apabila pada jangka waktu mulai dari pukul 11:58:00 sampai 12:00:00 (menjelang tengah hari dan tengah malam) komputer Anda akan melakukan *restart* sendiri, karena ini perbuatan BlueFantasy.

Yang juga tidak kalah menarik lagi adalah, apabila Anda memiliki perangkat CD/DVD writer pada Windows XP, virus ini akan menginfeksi direktori *temporary* dari CD Burning tersebut, di mana direktori ini merupakan tempat menyimpan file-file sementara yang nantinya akan di-*burning*.

Pesan dari Pembuat Virus

Virus ini juga menciptakan file dengan nama BlueFantasy.exe dan BlueFantasy.doc pada Desktop dan My Documents. Untuk BlueFantasy.doc attribut-nya diset sebagai *Hidden*, sehingga tidak terlihat.

Apabila Anda mengklik atau mengeksekusi file BlueFantasy.exe ini pada salah satu dari direktori tersebut, maka virus ini akan memanggil file BlueFantasy.doc yang ia sembunyikan tadi. Yang menarik dari file ini adalah terdapatnya lantunan syair yang dibuat oleh si empunya virus, yang sebenarnya diambil dari penggalan-penggalan judul lagu dari group band "Padi".

Bagaimana Cara Membasminya?

Jika komputer Anda memang sudah terserang virus ini, tidak perlu khawatir. Karena kami sudah meng-*update* database dari PC Media Antivirus, agar dapat mengenali dan membasmi virus ini secara tuntas. Hanya saja kami sarankan agar Anda mengubah kembali semua attribut file .doc menjadi normal, karena virus ini telah mengubahnya menjadi *hidden*. Caranya dengan mengaktifkan terlebih dahulu opsi "Show hidden files and folders" pada tab View di Folder Options. Setelah itu klik kanan file yang dimaksud dan nonaktifkan centangan (✓) untuk hidden. ■